Jacobi polynomials, certain elliptic modular forms and supersingular elliptic curves

AUTHOR(S):

金子, 昌信

数理解析研究所講究録
925巻 1995年 178-185

Jacobi polynomials, certain elliptic modular forms and supersingular elliptic curves.

京都工芸繊維大学工芸学部
金子昌信 (Kaneko, Masanobu)

§.0 Chebyshev 多項式

本題に入る前にChebyshev多項式について簡単に復習しておこう。

第1種および第2種Chebyshev多項式 $T_n(x)$, $U_n(x)$ とは n 次多項式 ($n=0,1,2,\cdots$) であって

$$T_n(\cos\theta)=\cos n\theta,\quad U_n(\cos\theta)=\frac{\sin(n+1)\theta}{\sin\theta}$$

をみたすものであった。はじめのいくつかをかくと,

n	0	1	2	3	4	5
$T_n(x)$	1	x	$2x^2-1$	$4x^3-3x$	$8x^4-8x^2+1$	$16x^5-20x^3+5x$
$U_n(x)$	1	$2x$	$4x^2-1$	$8x^3-4x$	$16x^4-12x^2+1$	$32x^5-32x^3+6x$

これらは直交関係

$$m\neq n \Rightarrow \int_{-1}^{1}\frac{1}{\sqrt{1-x^2}}T_m(x)T_n(x)\,dx=0,\quad \int_{-1}^{1}\sqrt{1-x^2}\,U_m(x)U_n(x)\,dx=0$$

をみたし, 所謂直交多項式の最も基本的な例となっている。数学に限らず, いろんな所に顔を出すようであるが, 数論で

は次のような結果がある（I. Schur; Arithmetisches über die Tschebyscheffschen Polynome", 全集 #84 (遺稿)).

Th (Schur)

i) $p = 2^n - 1 > 3$ が素数 $\iff T_{\frac{p+1}{4}}(2) \equiv 0 \mod p$

ii) $p = 2^{2n} + 1 > 5$ が素数 $\iff T_{\frac{p-1}{4}}(4) \equiv 0 \mod p$.

さて Chebyshev 多項式は Jacobi 多項式という超幾何多項式の特別な場合である。これを説明して主結果を述べる.

§. 1. Jacobi 多項式, 主結果

本質的には勿論同じことであるが, Jacobi がもともと考えた形の内積で2種類の Chebyshev を統一的に扱える。
Jacobi は "Untersuchungen über die Differentialgleichung der Hypergeometrischen Reihe" 全集 IV, pp 184~202 において, 多項式環 $\mathbb{R}[t]$ 上の内積

$$(f, g) := \int_0^1 t^\alpha (1-t)^\beta f(t) g(t)\, dt \qquad \alpha, \beta > -1$$

を考え, これに関する直交多項式が Gauss の超幾何微分方程式を満たすことを示した。

今特に $\alpha = -\frac{1}{a}$, $\beta = -\frac{1}{b}$ $a, b \geq 2, \in \mathbb{Z}$ とし,

$R[t]$ より広い

$$R[t^{1/a},(1-t)^{1/c}]=\bigoplus_{\substack{0\le\delta<a\\0\le\varepsilon<c}} t^{\frac{\delta}{a}}(1-t)^{\frac{\varepsilon}{c}}R[t]$$

上で上の内積を考える。その $t^{\frac{\delta}{a}}(1-t)^{\frac{\varepsilon}{c}}R[t]$ ($\simeq R[t]$) への制限は正定値であって，直交系

$\{t^{\frac{\delta}{a}}(1-t)^{\frac{\varepsilon}{c}}f_n^{(\delta,\varepsilon)}(t)\}_{n\ge 0}$，$f_n^{(\delta,\varepsilon)}(t)$ は n 次 monic 多項式，が定まる。Jacobi の結果をこの場合にあてはめれば，(拡大環を考えるといっても内積をシフトさせるだけなので)

Th (Jacobi) $f_n^{(\delta,\varepsilon)}(t)=(\text{const})\times F\left(-n,n+1+\frac{2\delta-1}{a}+\frac{2\varepsilon-1}{c};1+\frac{2\delta-1}{a};t\right)$.

ここに $F(\alpha,\beta,\gamma;x)=\sum_{i=0}^{\infty}\frac{\binom{-\alpha}{i}\binom{-\beta}{i}}{\binom{-\gamma}{i}}(-x)^i$

($\alpha=-n$ であるから n 次で切れて多項式となる)

例 $a=c=2$ のときが Chebyshev に外ならない。

(δ,ε)	$t^{\frac{\delta}{2}}(1-t)^{\frac{\varepsilon}{2}}f_n^{(\delta,\varepsilon)}(t)$	$t=x^2$, $\left(\begin{smallmatrix}t^{1/2}=\cos\theta\\(1-t)^{1/2}=\sin\theta\end{smallmatrix}\right)$
$(0,0)$	$1,\ t-\frac{1}{2},\ t^2-t+\frac{1}{8},\ t^3-\frac{3}{2}t^2+\frac{9}{16}t-\frac{1}{32},\ \cdots$	$2^{1-2n}T_{2n}(x)$
$(1,0)$	$t^{1/2},\ t^{3/2}-\frac{3}{4}t^{1/2},\ t^{5/2}-\frac{5}{4}t^{3/2}+\frac{5}{16}t^{1/2},\ \cdots$	$2^{-2n}T_{2n+1}(x)$
$(0,1)$	$(1-t)^{1/2}\times[1,\ t-\frac{1}{4},\ t^2-\frac{3}{4}t+\frac{1}{16},\ \cdots]$	$2^{-2n}U_{2n}(x)$
$(1,1)$	$(1-t)^{1/2}\times[t^{1/2},\ t^{3/2}-\frac{1}{2}t^{1/2},\ t^{5/2}-t^{3/2}+\frac{3}{16}t^{1/2},\ \cdots]$	$2^{-2n-1}U_{2n+1}(x)$

つまり $R[t^{1/2},(1-t)^{1/2}]$ を $\mathbb{Z}/2\times\mathbb{Z}/2$ の作用で分解したときの各成分に第1種，第2種の，even, odd Chebyshev 多項式が対応している。

我々の結果はChelyshevの次の場合，即ち $a=3$, $b=2$ のときである。

Theorem (with D. Zagier, vague form)
$a=3$, $b=2$ のときの $f_n^{(\delta,\varepsilon)}$ が supersingular j-polynomials を与える。

§2 supersingular 多項式

supersingular j-多項式とは，各素数 p に対して

$$SS_p(j) := \prod_{E:\text{S.S. ell}/\overline{\mathbb{F}_p}} (j - j(E))$$

で定義される多項式である。ここに積は $\overline{\mathbb{F}_p}$ 上の supersingular 楕円曲線の同型類（有限個）をわたり，$j(E)$ は E で代表される類の j-不変量である。$SS_p(j) \in \mathbb{F}_p[j]$ であって，$SS_2(j)=j$, $SS_3(j)=j$. 以後 $p \geq 5$ とする。いま

$$p-1 = 12n+4\delta+6\varepsilon, \quad n \geq 0, \ \delta \in \{0,1,2\}, \ \varepsilon \in \{0,1\}$$

と書く。（偶数 ≥ 4 はこの形に unique に書ける）。このとき $\deg SS_p(j) = n+\delta+\varepsilon$ であることは Deuring-Eichler により知られている。我々の定理の正確な形は次の通り。

Theorem (explicit form) $SS_p(j) = 1728^n \cdot j^\delta (j-1728)^\varepsilon f_n^{(\delta,\varepsilon)}\left(\frac{j}{1728}\right) \bmod p$
ただし $f_n^{(\delta,\varepsilon)}$ は $a=3$, $b=2$ のときのもの。 $(p \geq 5)$

証明には、$F = SS_p(j)/j^\delta(j-1728)^\varepsilon$ が2階の微分方程式（$\mathbb{F}_p$ 上）

$$(*)\quad j(j-1728)F'' + \{(\tfrac{1}{2}+\varepsilon)j + \tfrac{2}{3}(1+\delta)(j-1728)\}F' + (\tfrac{\delta\varepsilon}{3}+\tfrac{\delta}{6}+\tfrac{\varepsilon}{3}+\tfrac{1}{144})F = 0$$

を満たすことを用いる。このことは Igusa : Class number of a definite quaternion with prime discriminant, Proc. N.A.S. 44 (1958), 312-314 （λ-invariant の場合）以来 essential には知られている。又、(*) をそのまま $ch.=0$ で考えて、例えば $p\equiv 1 \pmod{12}$ ($\delta=\varepsilon=0$) なら

$SS_p(j) \equiv j^n F(\tfrac{1}{12}, \tfrac{5}{12}; 1; \tfrac{1728}{j})$ の多項式部分 $\bmod p$

などは知られていた（Carlitz ?）。ここでのポイントは (*) の係数 0 への持ち上げで、それ自身多項式解（Jacobi 多項式）をもつものが見つかったことにある。

この多項式（$a=3$, $k=2$ のときの $f_n^{(\delta,\varepsilon)}(t)$）は modular form の context から自然に導入することも出来る。それを次の §3 で説明しよう。

§3 modular form との関係

$SL_2(\mathbb{Z})$ 上の weight k ($k\geq 0$, even) の正則 modular forms の空間を M_k とする。先のごとく偶数 k を

$k = 12n + 4\delta + 6\varepsilon$, $n \geq -1$, $\delta \in \{0,1,2\}$, $\varepsilon \in \{0,1\}$ と書き表すと, $\mathbb{C}$-vectorspace M_k の次元は $\dim M_k = n+1$ で与えられる。今, 重さ2の derivation

$$\partial_k : M_k \longrightarrow M_{k+2}$$

を

$$\partial_k(f) := \frac{1}{2\pi i}\frac{df}{d\tau} - \frac{kE_2}{12} f$$

で定義する。ここに τ は上半平面上の変数で, 一般に k に対し $E_k(\tau) := 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$, $q = e^{2\pi i\tau}$ は Eisenstein 級数 (B_k は Bernoulli 数). $k \geq 4$ なら $E_k \in M_k$ であるが $E_2 \notin M_2 = \{0\}$ で, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ に対し

$$E_2\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 E_2(\tau) + \frac{6}{\pi i}c(c\tau+d)$$

となる. このように保型性がこわれていることと, $\frac{1}{2\pi i}\frac{d}{d\tau}$ $(= q\frac{d}{dq})$ が保型性を保たないことが打ち消し合って $\partial_k(f)$ は M_{k+2} に入ることが確かめられる。∂_k は人工的なものでなく, $\bigoplus_{k\geq 0} M_k$ 上の wt 2 の derivation で cusp forms の空間を保つものとして定数倍を除き unique に定まる。

さて2階の微分作用素

$$\partial_{k+2}\partial_k : M_k \longrightarrow M_{k+4}$$

を考えよう。M_k の次元公式から, $k \not\equiv 2 \pmod 3$ であれば

$\dim M_k = \dim M_{k+4}$, 従って $M_{k+4} = E_4 \cdot M_k$.

よってこのとき

$$\phi_k := \frac{1}{E_4}\partial_{k+2}\partial_k \in \mathrm{End}\, M_k.$$

この ϕ_k は cusp forms を保ち，q-展開の定数項を $k(k+2)/144$ 倍するから $k(k+2)/144$ が ϕ_k の1つの固有値．それに対応する固有関数を1つ，F_k，をとる．すると，$\partial(\Delta)=0$ （$\Delta=(E_4^3-E_6^2)/1728$．wt 12 の cusp form．$\partial=\partial_{12}$）ということより，$\Delta^i F_{k-12i}$，$1\leqq i\leqq n$ が ϕ_k の固有値 $(k-12i)(k-12i+2)/144$ の固有関数になることがわかる．従って ϕ_k は次元 $(=n+1)$ 個の相異なる固有値を持ち，F_k は定数倍を除き unique ということになる．その定数をあとの都合上

$$F_k(\tau)\text{の}q\text{-展開の定数項} = (-1)^n\binom{\frac{k-5}{6}}{n}$$

で normalize しておく．（ϕ_k の固有関数のうち，cusp form であるものは wt の低い固有関数に Δ の中をかけてえられるいわば "old forms" である．）

さて，k に対し n, δ, ε を先の通りとすると，

$F_k(\tau)/(\Delta^n E_4^\delta E_6^\varepsilon)$ は wt 0，上半平面上正則となって，従って $j=E_4^3/\Delta$ の多項式．それを $\widetilde{F_k}(j)$ と書く

Theorem $\widetilde{F_k}(j) = (-1728)^n\binom{\frac{k-5}{6}}{n} f_n^{(\delta,\varepsilon)}\left(\frac{j}{1728}\right)$．

ここに $f_n^{(\delta,\varepsilon)}$ は §1 の $a=3$, $b=2$ の場合の直交多項式

これをみるには、F_k のみたすてに関する微分方程式を $\widetilde{F}_k$ の j に関するそれに書き直せばよい。

Cor. 1　$p \geq 5$ 素数とすると、

$$SS_p(j) \equiv j^{\varepsilon}(j-1728)^{\delta}\widetilde{F}_{p-1}(j) \mod p$$

（$p-1 \not\equiv 2 \pmod 3$ 及び $k=p-1 \Rightarrow (-1)^n\binom{\frac{k-5}{6}}{n} \equiv 1 \mod p$ に注意）

Cor. 2　$\nu_0 = \frac{1}{3}(1-2\delta)$, $\nu_1 = \frac{1}{2}(1-2\varepsilon)$, $\nu_\infty = \frac{k+1}{6}$

$Y_0 = E_4^3$, $Y_1 = -E_6^2$, $Y_\infty = -1728\Delta$ とし、

σ を $\{0,1,\infty\}$ の任意の置換とすると

$$F_k(\tau) = \operatorname{sgn}(\sigma)^n E_4^{\delta} E_6^{\varepsilon} \sum_{i=0}^{n} (-1)^i \binom{n-\nu_{\sigma(0)}}{i}\binom{n-\nu_{\sigma(\infty)}}{n-i} Y_{\sigma(\infty)}^{i} Y_{\sigma(0)}^{n-i}$$

1) $\widetilde{F}_k(j)$ の超幾何表示を具体的に書き下す。その時、Kummer によって、みかけの異なる6通りの表示（24コのうち6コが多項式解を与える）を得、それが上の σ の6通りの置換に対応している。

§4　あとがき

以上、研究会で話したことのうち、以前の講究録（775, 844）に書いてあることは省いた残りを少し詳しくして書きました。